



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office

Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/724,949	10/02/96	CHEN	E

LM41/1230
NORMAN KLIVANS, ESQ.
SKJERVEN, MORRILL, MACPHERSON, FRANKLIN
& FRIEL
25 METRO DRIVE, SUITE 700
SAN JOSE CA 95110

EXAMINER
PALYS, J

ART UNIT	PAPER NUMBER
2785	5

DATE MAILED: 12/30/97

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.
08/724,949

Applicant(s)
Chen et al.

Examiner
Joseph Palys

Group Art Unit
2785



☒ Responsive to communication(s) filed on Oct 2, 1996

☐ This action is **FINAL**.

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire 3 month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) 1-35 is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) 1-22, 24-26, 28, 30-33, and 35 is/are rejected.

☒ Claim(s) 23, 27, 29, and 34 is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☒ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been
☐ received.

☐ received in Application No. (Series Code/Serial Number) _____

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

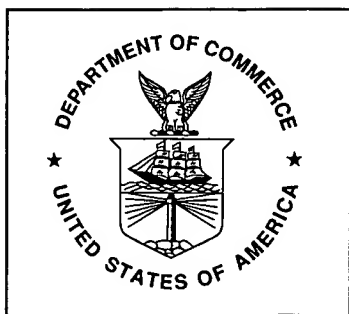
☐ Interview Summary, PTO-413

☒ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

☒ Exhibit A

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---



UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
ASSISTANT SECRETARY AND COMMISSIONER OF
PATENTS AND TRADEMARKS
Washington, D.C. 20231

EXAMINER: J. PALYS
ART UNIT: 2785
SERIAL NUMBER: 08/724,949

PART III. DETAILED ACTION

Drawings

1. This application has been filed with informal drawings which are acceptable for examination purposes only. Formal drawings will be required when the application is allowed.

Claim Rejections - 35 U.S.C. § 112

2. Claims 8,9,10,11 and 23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claim 8 recites the limitation "the first suspect instruction identifier" in line 3. There is insufficient antecedent basis for this limitation in the claim.

4. Claim 9 recites the limitation "the repaired macro" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim 10 is rejected because of their dependency of claim 8, rejected above.

5. Claim 11 recites the limitation "the second suspect instruction identifier" in line 3. There is insufficient antecedent basis for this limitation in the claim.

6. Claim 23 recites the limitation "the treated macro" in line 5. There is insufficient antecedent basis for this limitation in the claim.

Art Unit: 2785

7. Claims 13,14,20,22,28,30 are rejected under 35 U.S.C. 112, first paragraph, because the specification, while being enabling for suspect instruction identifiers comprising of the string 73 CB 00 0C 6C 01 00, it does not reasonably provide enablement for strings of 67 C2 80, and 64 6F 02 67 DE 00 73 87 01 12 73 7F, and. 6D 61 63 72 6F 73 76 08, and 12 6C 01 00, and 64 67 C2 80 6A 0F 47, and 79 7C 66 6F 72 6D 61 74 20 63 6A, and 80 05 6A 07 43 4F 4D. The specification does not enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to use the invention commensurate in scope with these claims. Page 28 of the applicant's disclosure specifically mentions the string 73 CG 00 6C 01 00 corresponding to the portion .format =1. The disclosure fails to provide any description of the instructions associated with the strings described in the above referenced claims.

Claim Rejections - 35 U.S.C. § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Note regarding effective date of the Bontchev reference.

Due to the lack of an exact date of publication, other than the year, printed on the Bontchev reference, attached to the action is Exhibit A which provides information regarding the effective date of the article written by Bontchev. The author states in Exhibit A that he believes the publication date to be September of 1996. He also admits to providing the article to the publisher in July of 1996, which satisfies the requirement of 35 U.S.C. 102(a), from which the information was known to "others".

Art Unit: 2785

9. Claims 1-8,10-12,15-19,21,24-26,31-33,35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bontchev "POSSIBLE MACRO VIRUS ATTACKS AND HOW TO PREVENT THEM" in view of Arnold et al., U.S. Patent No. 5,440,723.

Bontchev teaches a method of detecting macro viruses in selected files, such that the files can be corrected or removed. The methods include the use of comparison data for detecting a virus, such that a macro is retrieved, and scanned for presence of the comparison data. Upon recognition of such comparison data, the macro is considered as a possible or definite infected software entity. (see entire document, specifically sections 2.1-2.1.2, page 602, second column 4th full ppg, , sections 2.1.5 to 2.1.6, 2.2, 2.2.2 to 2.2.3, page 611, second column, second full ppg, sections 3.2 and 4).

As per claim 1, Bontchev does not specifically show the decoding of the macro's and using the decoded macro to be compared to comparison data, nor the specifics of a computer system implementing the method.

As per the computer system, it would have been obvious to one of ordinary skill in the art to realize that the methods and functions described in Bontchev's paper is clearly bounded around a computer system which essentially includes at the very least a processor and memory, to execute the software described in his paper. Accordingly, it would have been obvious to one of ordinary skill in the art to allow a computer system to execute the above functions.

Arnold teaches a virus detection system which allows a target file or location to be scanned for likeliness of viral signatures. The system allows the target file to be "decoded" such that the target file is scanned via byte sized blocks, and compared to known comparison signatures for coincidence. Upon a match, the virus is removed, as well as collected for future references. (column 5 lines 28-68 and column 7

Art Unit: 2785

line 10 to column 8 line 16 and column 9 line 11 to column 10 line 10 and column 17 line 35 to column 19 line 44).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow Bontchev's teachings to utilize the signature scanning features taught by Arnold because it would enable for his virus detecting methods to utilize procedures which are known to recognize viral activity, thus enabling the macro to be either corrected or removed, thus eliminating the propagation of the virus. This would have been obvious because Bontchev suggests use of such scanning methods using analyzers which allow certain macro's with possible infections to be located, (page 602, second column fourth full ppg, page 604, first column, second full ppg, page 608, first column, first full ppg, and section 2.3, page 611, second column second full ppg). Thus, one of ordinary skill in the art would have recognized these suggestions along with the teachings of Arnold, and have been motivated to allow the macro's to be "decoded" in that they are broken down into blocks of information from which viral signatures can be compared to them to detect possible infections. This would have been obvious because both Bontchev and Arnold are directed toward the detection and correction of virus infected software entities, and one of ordinary skill in the art would have recognized these similarities and concluded that they are from the same field of endeavor. Accordingly, it would have been obvious to one of ordinary skill in the art to allow the scanning and detection functions taught by Arnold to be incorporated into a macro virus detection system, in order to allow this type of virus to be found and removed in a computer system.

As per claim 2, Bontchev suggest the correction of the macro's after a detection of a virus (see previous citations) however, he does not specifically state removing the virus, although inferred.

Arnold teaches removing a detected virus once it has been detected, from an infected software entity. (column 5 lines 59-68).

Art Unit: 2785

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow Bontchev's combined system with Arnold, to remove a detected virus from an infected macro because it would ensure that the system the macro is working in does not propagate the infection. This would have been obvious because not only does Bontchev suggest the correction of macro's after a viral detection, one of ordinary skill in the art would have found it obvious to realize that removing the virus is an obvious function that would need to be done in order to make the viral detection process actually useful, as shown by Arnold. That is, one of ordinary skill in the art would have found it useless to employ a viral detection process without correcting and removing the virus once its was detected. Accordingly, it one of ordinary skill in the art would have been motivated to remove a virus from an infected macro, one the detection mechanisms discussed above, located one in the target system.

As per claim 3, Bontchev suggests the retrieving of a macro by locating template files, as well determining whether an embedded macro is found within the target system as well. (page 607, section 2.2.2 to page 608, section 2.2.3, page 610 to page 616) Accordingly, the macro within the template file, or any other located macro would be subject to the same scrutiny as any other macro scanned or processed, by the viral detection functions described by Bontchev. This would have been an obvious observation because Bontchev teaches the scanning or locating of macro's within the target system, thus locating embedded macro's and or template files would have been an obvious feature of the above process to ensure that all macro's within the system are virus free.

As per claims 4,5 and 12, Bontchev does not show the use of first and second instruction identifiers.

Arnold teaches the ability to utilize a plurality of suspect identifiers as the comparison data. (column 9 line 13 to column 10 line 10). Arnold teaches the labeling of a virus only when a number of the portions are found in the target entity, (column 9 lines 30-34).

Art Unit: 2785

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow the combined system of Bontchev and Arnold to utilize a plurality of portions of suspect identifiers when scanning the macro because it reduces the number of "false positives" during the identifying process, which reduces the processing of non viral activities. This would have been obvious because Bontchev suggests the concern for "false positives" as well as "negatives" in his paper (page 604, section 2.1.6 and page 611 second column, second full ppg), thus one of ordinary skill in the art would have recognized this, along with Arnold's teachings, and allowed this concern to be addressed by ensuring that a number, in this case two, identifiers being located within the target entity (macro) before declaring it as infected. As per the identifiers being "instruction" identifiers, it would have been obvious to one of ordinary skill in the art to realize that the signatures extracted from the target entity are strings of bytes, which correspond to the code within the software program being scanned. This program inherently include instructions, thus the signatures extracted, and subsequently logged in a data base for future comparison, would be considered instruction identifiers as well.

Furthermore, Bontchev teaches the ability to identify "instructions" associated with the macro's which may include viruses, thus one of ordinary skill in the art would have been motivated to incorporate the "false positive" theme of recognizing more than one identifier before labeling a virus, as taught by Arnold, with the locating macro instructions, for the reasons set forth above.

As per claims 6 and 7, Bontchev suggest the macro viruses including enablement and reproduction qualities, (instructions) and suggests techniques of detecting such qualities. (pages 604-605, section 2.1.6, pages 607-608, section 2.2.3, page 612, section 2.3.4, and 2.3.5 and pages 613-614, section 2.3.6). The macro viruses described by Bontchev include the qualities of reproduction and execution (enablement) within the macro's they infect. Accordingly, it would have been obvious to one of ordinary skill in the art to realize

Art Unit: 2785

that the suspect identifiers used in scanning and locating these macro viruses would include these qualities as well, in order to detect them, and correct the infected entity. One of ordinary skill in the art would have found this obvious because the combined system of Bontchev and Arnold is constructed for the purpose of locating macro viruses which perform the characteristics described by Bontchev, and allowing the comparison identifiers to include the reproduction and enablement characteristics (i.e associated instructions which form these macros) would have been an obvious implementation, for the detection reasons set forth previously.

As per claims 8 and 11, as previously described, Arnold teaches the removal of viruses from the infected target system, after detection using suspect identifiers, (column 9 line 13 to column 10 line 10), and although Bontchev does not specifically describe this, it would have been obvious to one of ordinary skill in the art to realize that once the virus associated with the identifier's was located, the removal process taught by Arnold, would include this associated suspect portion of the target entity. This would have been obvious because, the removal process suggested by Arnold allows the viral entity to be removed from the target system, and one of ordinary skill in the art would have realized that this would include any portions of the virus, including the portions found to be suspect due to the comparison techniques suggested by both references. The same goes for locating additional identifiers, and suspect portions in the target entity, as claimed in claim 11. As per the use of additional identifiers to locate a virus, Arnold does teach the use of a plurality of identifiers to ensure a correct detection. (column 9 lines 30-34).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow the combined system of Bontchev and Arnold to utilize a plurality of portions of suspect identifiers when scanning the macro because it reduces the number of "false positives" during the identifying process, which reduces the processing of non viral activities. This would have been obvious because Bontchev suggests the concern for "false positives" as well as "negatives" in his paper (page 604, section 2.1.6 and

Art Unit: 2785

page 611 second column, second full ppg), thus one of ordinary skill in the art would have recognized this, along with Arnold's teachings, and allowed this concern to be addressed by ensuring that a number, in this case two, identifiers being located within the target entity (macro) before declaring it as infected. As per the identifiers being "instruction" identifiers, it would have been obvious to one of ordinary skill in the art to realize that the signatures extracted from the target entity are strings of bytes, which correspond to the code within the software program being scanned. This program inherently include instructions, thus the signatures extracted, and subsequently flogged in a data base for future comparison, would be considered instruction identifiers as well. Furthermore, Bontchev teaches the ability to identify "instructions" associated with the macro's which may include viruses, thus one of ordinary skill in the art would have been motivated to incorporate the "false positive" theme of recognizing more than one identifier before labeling a virus, as taught by Arnold, with the locating macro instructions, for the reasons set forth above.

As per claim 10, although not specifically stated, the replacement of faulty, or infected portions, or instructions, with no op or benign instructions or portions, is a notoriously well known concept in the art, and allowing the combined system of Bontchev and Arnold to utilize such correction techniques while removing viruses from a target file (macro) would have been an obvious variation and implementation of well known correction techniques. One of ordinary skill in the art would have recognized the well known advantages of replacing faulty or infected portions of a target file with no ops, as is known in the art, and thus have been motivated to allow such advantages to be incorporated into the combined system above, to allow the target file to not to be rendered completely useless because of a portion of infection.

As per claims 15,24,31 and 35, Bontchev teaches a method of detecting macro viruses in selected files, such that the files can be corrected or removed. The methods include the use of comparison data for detecting a virus, such that a macro is retrieved, and scanned for presence of the comparison data. Upon

Art Unit: 2785

recognition of such comparison data, the macro is considered as a possible or definite infected software entity. (see entire document, specifically sections 2.1-2.1.2, page 602, second column 4th full ppg, , sections 2.1.5 to 2.1.6, 2.2., 2.2.2 to 2.2.3, page 611, second column, second full ppg, and sections 3.2 and 4).

As per claims 15,24,31 and 35, Bontchev does not specifically show the decoding of the macro's and using the decoded macro to be compared to comparison data, nor the specifics of a computer system implementing the method.

As per the computer system in claim 15, it would have been obvious to one of ordinary skill in the art to realize that the methods and functions described in Bontchev's paper is clearly bounded around a computer system which essentially includes at the very least a processor and memory, to execute the software described in his paper. Accordingly, it would have been obvious to one of ordinary skill in the art to allow a computer system to execute the above functions.

Arnold teaches a virus detection system which allows a target file or location to be scanned for likeliness of viral signatures. The system allows the target file to be "decoded" such that the target file is scanned via byte sized blocks, and compared to known comparison signatures for coincidence. Upon a match, the virus is removed, as well as collected for future references. (column 5 lines 28-68 and column 7 line 10 to column 8 line 16 and column 9 line 11 to column 10 line 10 and column 17 line 35 to column 19 line 44).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow Bontchev's teachings to utilize the signature scanning features taught by Arnold because it would enable for his virus detecting methods to utilize procedures which are known to recognize viral activity, thus enabling the macro to be either corrected or removed, thus eliminating the propagation of the virus. This would have been obvious because Bontchev suggests use of such scanning methods using analyzers which

Art Unit: 2785

allow certain macro's with possible infections to be located, (page 602, second column fourth full ppg, page 604, first column, second full ppg, page 608, first column, first full ppg, and section 2.3, page 611, second column second full ppg). Thus, one of ordinary skill in the art would have recognized these suggestions along with the teachings of Arnold, and have been motivated to allow the macro's to be "decoded" in that they are broken down into blocks of information from which viral signatures can be compared to them to detect possible infections. This would have been obvious because both Bontchev and Arnold are directed toward the detection and correction of virus infected software entities, and one of ordinary skill in the art would have recognized these similarities and concluded that they are from the same field of endeavor. Accordingly, it would have been obvious to one of ordinary skill in the art to allow the scanning and detection functions taught by Arnold to be incorporated into a macro virus detection system, in order to allow this type of virus to be found and removed in a computer system.

As per claims 15,24,31 and 35, Bontchev does not show the use of first and second instruction identifiers.

Arnold teaches the ability to utilize a plurality of suspect identifiers as the comparison data. (column 9 line 13 to column 10 line 10). Arnold teaches the labeling of a virus only when a number of the portions are found in the target entity, (column 9 lines 30-34).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow the combined system of Bontchev and Arnold to utilize a plurality of portions of suspect identifiers when scanning the macro because it reduces the number of "false positives" during the identifying process, which reduces the processing of non viral activities. This would have been obvious because Bontchev suggests the concern for "false positives" as well as "negatives" in his paper (page 604, section 2.1.6 and page 611 second column, second full ppg), thus one of ordinary skill in the art would have recognized this,

Art Unit: 2785

along with Arnold's teachings, and allowed this concern to be addressed by ensuring that a number, in this case two, identifiers being located within the target entity (macro) before declaring it as infected. As per the identifiers being "instruction" identifiers, it would have been obvious to one of ordinary skill in the art to realize that the signatures extracted from the target entity are strings of bytes, which correspond to the code within the software program being scanned. This program inherently include instructions, thus the signatures extracted, and subsequently flogged in a data base for future comparison, would be considered instruction identifiers as well. Furthermore, Bontchev teaches the ability to identify "instructions" associated with the macro's which may include viruses, thus one of ordinary skill in the art would have been motivated to incorporate the "false positive" theme of recognizing more than one identifier before labeling a virus, as taught by Arnold, with the locating macro instructions, for the reasons set forth above.

As per claims 24,31 and 35 specifically, Bontchev does not specifically show the structure of a virus information module which stored the comparison data, and a scanning module to perform the scanning functions suggested in his teachings.

Arnold teaches the use of a virus detection system which includes a storage module (database) for storing comparison data (the identifiers) as well as a scanning module to perform the comparison techniques described above. (Figure 1a and 8, column 27 line 15 to column 29 line 40). As per claim 35, although the scanner is not specifically labeled as a processor, it would have been obvious to one of ordinary skill in the art to realize that the functions performed by it are essentially similar to processing of information, (i.e. the comparison functions, etc.). Accordingly, it would have been obvious to one of ordinary skill in the art to utilize a processor in the scanner in order to allow these functions to be performed quickly and accurately, as is a known advantages of processors, and their capabilities.

Art Unit: 2785

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow the features and functions described by Bontchev to be incorporated within a computer system which uses the virus detecting modules taught by Arnold, because it would allow dedicated system, comprising of the above noted elements, to be present for performing the virus scanning and detection procedures described above. This would have been obvious because it is clear that Bontchev's functions, along with Arnold's, are performed by some sort of "module" which allows the comparison and scanning techniques to take place, and allowing specific modules, such as those taught by Arnold, to be incorporated to perform these functions, would have been an obvious implementation of elements needed to ensure the macro virus techniques are carried out appropriately.

As per claim 16, Bontchev and Arnold both teach treating an infected entity (macro) when a virus is determined to be present, which in the case above, would include the determination of both identifiers in the target entity. (see previous citations for Bontchev and column 5 lines 59-68, for Arnold.).

As per claims 17,18,26 and 32, as previously described, Arnold teaches the removal of viruses from the infected target system, after detection using suspect identifiers, (column 9 line 13 to column 10 line 10), and although Bontchev does not specifically describe this, it would have been obvious to one of ordinary skill in the art to realize that once the virus associated with the identifier's was located, the removal process taught by Arnold, would include this associated suspect portion of the target entity. This would have been obvious because, the removal process suggested by Arnold allows the viral entity to be removed from the target system, and one of ordinary skill in the art would have realized that this would include any portions of the virus, including the portions found to be suspect due to the comparison techniques suggested by both references. The same goes for locating additional identifiers, and suspect portions in the target entity, as claimed in claim 18. As per the use of additional identifiers to locate a virus, Arnold does teach the use of a

Art Unit: 2785

plurality of identifiers to ensure a correct detection. (column 9 lines 30-34). As per claims 26 and 32, and the use of "modules" to perform these functions, it would have been obvious to one of ordinary skill in the art to realize that some sort of element has to be present or utilized to perform these functions, and allowing Bontchev's system to make use of such elements would have been an obvious implementation of such elements, to ensure that these features are performed correctly. This would have been obvious because Arnold shows the use of modules that perform the needed functions in his virus detection system, thus one of ordinary skill in the art would have found it obvious to utilize components that are connected for proper communications, (i.e the database, scanning module etc.) to perform the above noted functions taught by the combined system, in order to ensure they are implemented correctly.

As per claim 19, Bontchev suggests the retrieving of a macro by locating template files, as well determining whether an embedded macro is found within the target system as well. (page 607, section 2.2.2 to page 608, section 2.2.3, page 610 to page 616) Accordingly, the macro within the template file, or any other located macro would be subject to the same scrutiny as any other macro scanned or processed, by the viral detection functions described by Bontchev. This would have been an obvious observation because Bontchev teaches the scanning or locating of macro's within the target system, thus locating embedded macro's and or template files would have been an obvious feature of the above process to ensure that all macro's within the system are virus free.

As per claim 21, see the rejection to claim 15, as it discusses the use of a plurality of suspect identifiers (i.e. first and second identifiers).

As per claim 25, Bontchev suggests the retrieving of a macro by locating template files, as well determining whether an embedded macro is found within the target system as well. (page 607, section 2.2.2 to page 608, section 2.2.3, page 610 to page 616) Accordingly, the macro within the template file, or any other

Art Unit: 2785

located macro would be subject to the same scrutiny as any other macro scanned or processed, by the viral detection functions described by Bontchev. This would have been an obvious observation because Bontchev teaches the scanning or locating of macro's within the target system, thus locating embedded macro's and or template files would have been an obvious feature of the above process to ensure that all macro's within the system are virus free. Again, as per the use of "modules" to perform these functions, it would have been obvious to one of ordinary skill in the art to realize that some sort of element has to be present or utilized to perform these functions, and allowing Bontchev's system to make use of such elements would have been an obvious implementation of such elements, to ensure that these features are performed correctly. This would have been obvious because Arnold shows the use of modules that perform the needed functions in his virus detection system, thus one of ordinary skill in the art would have found it obvious to utilize components that are connected for proper communications, (i.e the database, scanning module etc.) to perform the above noted functions taught by the combined system, in order to ensure they are implemented correctly.

As per claim 33, Bontchev teaches the ability to recognize when a macro is in a target file (sections 2.1-2.1.2, page 602, second column 4th full ppg, , sections 2.1.5 to 2.1.6, 2.2., 2.2.2 to 2.2.3, page 611, second column, second full ppg, and sections 3.2 and 4).

Allowable Subject Matter

10. Claims 9,13,14,20,22,28,30 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112 set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Art Unit: 2785

11. Claims 23,27,29,34 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

12. The following is a statement of reasons for the indication of allowable subject matter:

The prior art fails to teach or suggest the method of claim 8, including the steps of verifying the integrity of the treated macro and replacing the infected macro in a targeted file with "the" repaired macro dependent upon the integrity verification of the treated macro, as claimed in claim 9.

The prior art fails to teach or suggest the set of identifiers including the specific strings identified in claims 13,14, 20,22,28 and 30 as well.

The prior art also fails to teach or suggest the method which allows the accessing of a targeted file, locating the macro within the targeted file, removing the macro from the targeted file and adding "the" treated macro to the targeted file to produce a corrected file, as specifically claimed in claim 23.

The prior art fails to teach or suggest the system of claim 26 including a file correcting module in communication with the macro treating module, for accessing of a targeted file, locating the macro within the targeted file, removing the macro from the targeted file and adding "the" treated macro to the targeted file to produce a corrected file, as specifically claimed in claims 27 and 34.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Palys whose telephone number is (703) 305-9685. The examiner can normally be reached Monday-Thursday from 6:30 AM to 4:00 PM. The examiner can also be reached on alternate Fridays.

Art Unit: 2785

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert Beausoliel, can be reached at (703) 305-9713. The fax number for this Group is (703) 305 9724.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-9618.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

or faxed to:

(703) 308-9051, (for formal communications intended for entry)

Or:

(703) 305-9724, (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA., Sixth Floor (Receptionist).

J.Palys
December 21, 1997



JOSEPH PALYS
PATENT EXAMINER
GROUP 2400

Exhibit A

Palys, Joseph

From: Harrity, John
Sent: Friday, December 19, 1997 9:37 AM
To: Palys, Joseph
Subject: FW: Published article

From: bontchev@complex.is[SMTP:bontchev@complex.is]
Sent: Friday, December 19, 1997 7:20 AM
To: Harrity, John
Subject: Re: Published article

> have a copy of an article you wrote, which was published in the
> magazine, COMPUTER & SECURITY, vol. 15, No. 7, pp. 595-626, 1996,
> entitled, "Possible macro virus attacks and how to prevent them".
>
> I need to know what month that article was published.

It was published in September 1996, I think. C&S publishes 10 issues per year.

> as well as any other information regarding when this article was
> submitted to the magazine,

It was submitted by the end of July 1996.

> Additionally, If you have any additional publications on "Macro
> Viruses", reference to these would also be greatly appreciated.

My paper submitted to the 7th International Virus Bulletin conference (San Francisco, October 1997) titled "Macro Virus Identification Problems" is available in electronic form from

<ftp://ftp.informatik.uni-hamburg.de/pub/virus/texts/viruses/macidpro.zip>

Regards,
Vesselin

--
Vesselin Vladimirov Bontchev, not speaking for FRISK Software International,
Posthof 7180, IS-127, Reykjavik, Iceland producers of F-PROT.
e-mail: bontchev@complex.is, tel.: +354-561-7273, fax: +354-561-7274
PGP 2.6.2i key fingerprint: E5 FB 30 0C D4 AA AB 44 E5 F7 C3 18 EA 2B AE 4E